



TITLE:

$M_{24} \sim M(I)$ (代数的組合せ論)

AUTHOR(S):

北詰, 正顕; 宮本, 雅彦

---

CITATION:

北詰, 正顕 ...[et al].  $M_{24} \sim M(I)$ (代数的組合せ論). 数理解析研究所講究録 1996, 962: 1-18

ISSUE DATE:

1996-08

URL:

<http://hdl.handle.net/2433/60549>

RIGHT:

# $M_{24} \sim M(I)$

北詰正顕 (千葉大理)・宮本雅彦 (愛媛大理)

連名による 3 回講演 (の報告) の第 1 回として, Mathieu 群から Conway 群を経て Monster へ至るまでの概観的な話をしようと思う。内容としては, Mathieu 群, Conway 群のさまざまな構成法を紹介し, その延長として Monster への approach の一例を紹介することである。すなわち, 宮本氏の結果 [17] の中で与えられた Lorentzian lattice の 21 個の reflections (これらの生成する群の商群が Monster になる) の具体像を与えようと思う。

全般にわたる参考文献として

[CS] J.H.Conway, N.J.A.Sloane: Sphere Packings, Lattices and Groups, Springer

を挙げておく。Mathieu 群, Conway 群については, [CS]10 章 (= [1]) が最も知られた論文だろう。邦文では, 近藤先生による講義録 [22] がある。

なお, この報告ならびに講演についての責は, すべて北詰にあることを記しておく。

## 1 The Mathieu Group $M_{24}$

24 次の Mathieu 群  $M_{24}$  を構成することについては, すでに標準的なものが確立しているという気がする。すなわち, 次の 2 つのいずれかを与えるというものである。

(A) Steiner System  $S(24, 8, 5)$

(B) Golay Code  $C_{24}$

まず, これら 2 つを (簡単に) 定義を与えておく。

(A) Steiner System  $S(24, 8, 5)$

$\Omega$  を 24 点からなる集合,  $\mathcal{O}$  を  $\Omega$  に含まれるいくつかの 8 点集合の族とする。このとき,

$\Omega$  に含まれる任意の 5 点集合  $S$  を含む  $\mathcal{O}$  の元がただひとつ存在する

が成り立つならば,  $(\Omega, \mathcal{O})$  は Steiner System  $S(24, 8, 5)$  をなすという。これは, 同型を除いて一意に定まる。

このとき,  $\mathcal{O}$  の各元は octad と呼ばれる。octad の総数 (i.e.  $|\mathcal{O}|$ ) は 759 であることが, 上記の性質から容易に得られる。

(B) Golay Code  $C_{24}$

Golay Code  $C_{24}$  は長さ 24 の binary code (すなわち,  $F_2^{24}$  の部分空間) で

self-dual ( $C_{24} = C_{24}^\perp$  (直交補空間))

doubly even (任意の  $w \in C_{24}$  に対し, その weight(後述)  $wt(w)$  は 4 の倍数)

minimum weight = 8 ( $C_{24}$  の零ベクトル以外の元の weight は 8 以上)

をみたすものである (同型を除いて一意に定まる)。ただし,  $w$  の weight とは  $w$  の 0 でない成分の個数である。

なお (A) との関連のこともあって  $F_2^{24}$  を  $\mathcal{P}(\Omega)$  ( $\Omega$  の部分集合全体) と同一視しておく。  $\mathcal{P}(\Omega) \ni A, B$  に対し, その和は  $A + B = (A \cup B) \setminus (A \cap B)$  で定義する。このとき weight とは, その部分集合の濃度を意味する。

さて,  $C_{24}$  の元 ( $\Omega$  のある部分集合) を  $\mathcal{C}$ -set と呼ぶ。  $\mathcal{C}$ -set の weight は 0, 8, 12, 16, 24 のいずれかになる。すぐ後で述べるように, weight 8 の元が (A) の octad に対応する。また weight 12 の元を dodecade とよぶことにする。これは,  $M_{12}$  との関連において重要である。

さて, (A) と (B) とは数学的には同値である。すなわち, (A) が与えられれば  $\mathcal{P}(\Omega)$  の部分空間 ( $\mathcal{O} \in \mathcal{O}$ ) を作ることで  $C_{24}$  が得られる。逆に  $C_{24}$  からは,  $\mathcal{O} = \{w \in C_{24} \mid |w| = 8\}$  により  $S(24, 8, 5)$  が構成される。

問題の Mathieu 群は, これらの全自己同型群として定義される。

$$M_{24} := \text{Aut } S(24, 8, 5) = \text{Aut } C_{24}$$

ただし, 自己同型とは ((A), (B) 共に)  $\Omega$  上の置換群で  $\mathcal{O}$  もしくは  $C_{24}$  を不変にするものをいう。

以上のことを踏まえた上で  $M_{24}$  の構成法をいくつか並べておこう。ひとつひとつの記述は短いコメントにとどめるがお許しいただきたい。(なお, 以下の表題の末尾には構成において数 24 がどのような形で現れるかを付記した。それぞれの構成のなかで, 数 24 が様々な意味を持つことがわかると思う。)

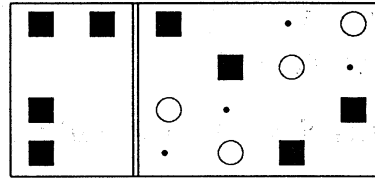
## 1.1 Extended Binary Golay Code (24=23+1)

$F_{23}$  の平方元の集合と, その平行移動 ( $F_{23}$  の元を足したもの) から (いわゆる Quadratic residue code として) Binary Golay Code を構成し, それを拡大したものが  $C_{24}$  になる。(だから extended とつけるのが正確な用語ではあるが, 省略することも多い。) 群構造としては  $L_2(23) \subset M_{24}$  という包含関係がこれを反映している。

Golay code を構成する最も標準的な方法であり, [1] にある。

## 1.2 MOG (Miracle Octads Generators) (24 = 8 + 16)

Curtis による非常に便利な構成法で, 一言で言ってしまうと  $\mathcal{O}$  のすべてを読み取れるようなひとつの表であり, 下のような図形が 35 個並んでいるものである。



この  $4 \times 6$  の長方形が  $\Omega$  の 24 点を表しており、例えば 8 個の ■ がひとつの octad を作る。  
 具体的な細かい計算をするには最も有用であり、[6] の表を何度利用したかわからない。  
 $\Omega$  の点をどう並べたらよいかという問いの答は [22] にある。

### 1.3 The Hexacode

(24=4×6)

4 元体  $F_4$  上のコード

$$\mathcal{H}_6 = \left\{ (h_1, \dots, h_6) \in F_4^6 \mid \begin{pmatrix} h_4 \\ h_5 \\ h_6 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ \omega^2 & \omega & 1 \\ \omega & \omega^2 & 1 \end{pmatrix} \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix} \right\}$$

から、 $\mathcal{C}_{24}$  を作る方法。MOG の表の 6 つの列が  $F_4^6$  の 6 つの成分に、4 つの行が  $F_4$  の 4 つの元  $(0, 1, \omega, \omega^2)$  に対応しており、■ の octad は  $(1, 0, 0, 1, \omega^2, \omega) \in \mathcal{H}_6$  から得られる。

[CS]11 章が演習問題付きで面白い。[14] では、この構成が（数学的に）役に立った。

### 1.4 Transitive Extensions

(24=21+1+1+1)

射影線形群  $L_3(4)$  の 2 重可移表現から、可移拡大を繰り返して  $L_3(4) \subset M_{22} \subset M_{23} \subset M_{24}$  という tower が得られる。これに対応して、 $L_3(4)$  が作用する射影平面からデザインの拡大として Steiner system  $S(22, 6, 3)$ ,  $S(23, 7, 4)$ ,  $S(24, 8, 5)$  が得られる。

置換群、デザイン、という観点から最も標準的な構成法である。[23],[21] に詳しい記述がある。

### 1.5 The Steiner System $S(12, 6, 5)$

(24=12+12)

$M_{24}$  を  $S(24, 8, 5)$  の全自己同型群として考えるとき、ひとつの dodecade の固定部分群は小さい方の Mathieu 群  $M_{12}$  になる。このとき dodecade には全体と同様に Steiner system  $S(12, 6, 5)$  の構造が入る。

このことの逆をたどって  $S(12, 6, 5)$  から  $S(24, 8, 5)$  を構成する方法があるが、それは  $M_{12}$  についてある程度述べた後で説明することにする。

## 2 The Small Mathieu Group $M_{12}$

小さい方の Mathieu 群  $M_{12}$  についても簡単に触れておく。 $M_{24}$  と同じように次のいずれかを考え、その全自己同型群として構成される。

### (A) The Steiner System $S(12, 6, 5)$

12 点集合  $\Delta$  と,  $\Delta$  の 6 点集合の族  $\mathcal{H}$  で

$\Delta$  に含まれる任意の 5 点集合  $S$  を含む  $\mathcal{H}$  の元がただひとつ存在する

が成り立つとき,  $(\Delta, \mathcal{H})$  は  $S(12, 6, 5)$  をなすという。

このとき,  $\mathcal{H}$  の各元は hexad と呼ばれ, その総数は 132 である。この数字が  $2 \times \binom{12}{2}$  に一致していることが後で大きな意味を持つ。

### (B) The Ternary Golay Code $\mathcal{C}_{12}$ ( $\subset \mathbb{F}_3^{12}$ )

3 元体上の self-dual, even かつ minimal weight = 6 をみたす code である。全自己同型群は  $2.M_{12}$  となる。中心は  $\pm 1$  倍であり, (A) には現れないものである。

全自己同型群からもわかるように (A), (B) が同等というわけではない。ただし,  $\mathcal{C}_{12}$  が与えられれば,

$$\mathcal{H} = \{\text{supp}(w) \mid |w| = 6, w \in \mathcal{C}_{12}\}$$

により,  $S(12, 6, 5)$  が構成できる。

これらについてもいくつかの構成法が存在する。

## 2.1 Extended Ternary Golay Code

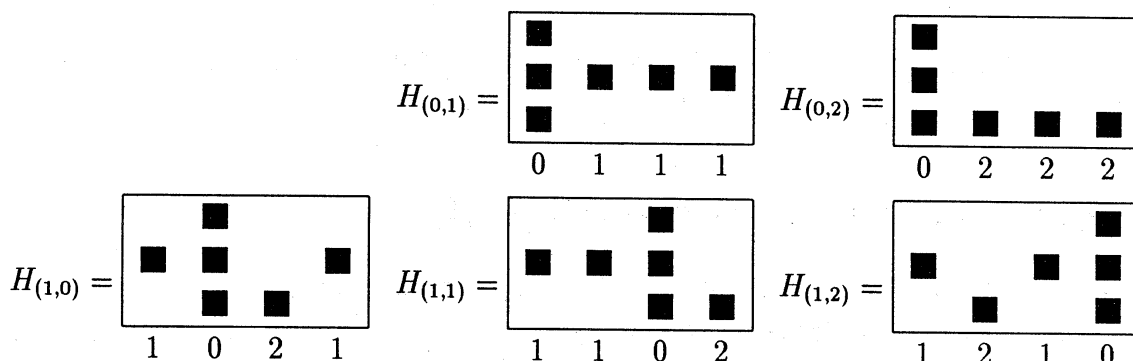
1.1 節と同様のことを,  $\mathbb{F}_3$  上で  $\mathbb{F}_{11}$  から始めることにより  $\mathcal{C}_{12}$  が構成される。[CS]3 章に定義が載っている。

## 2.2 Tetra Code

Tetra code とは,

$$\mathcal{T}_4 := \{(a, b, b - a, a + b) \mid a, b \in \mathbb{F}_3\}$$

で定義される小さなコードである。12 点集合  $\Delta$  は  $3 \times 4$  の長方形 (これを MOG に対応して MINIMOG とよぶ) に並んでいて, 3 つの行が  $\mathbb{F}_3$  の 3 つの元  $\{0, 1, 2\}$  に, 4 つの列が  $\mathcal{T}_4$  の 4 つの成分に対応している。 $\mathcal{T}_4$  の 0 でないベクトル  $(a, b, b - a, a + b)$  に対し,  $\Delta$  の 6 点集合  $H_{(a,b)}$  を次のように定義する。



$$\begin{array}{ccc}
 H_{(2,0)} = \begin{array}{|c|c|c|c|} \hline & \blacksquare & & \\ \hline & \blacksquare & \blacksquare & \\ \hline \blacksquare & \blacksquare & & \blacksquare \\ \hline 2 & 0 & 1 & 2 \\ \hline \end{array} &
 H_{(2,1)} = \begin{array}{|c|c|c|c|} \hline & & & \blacksquare \\ \hline & \blacksquare & & \blacksquare \\ \hline \blacksquare & & \blacksquare & \blacksquare \\ \hline 2 & 1 & 2 & 0 \\ \hline \end{array} &
 H_{(2,2)} = \begin{array}{|c|c|c|c|} \hline & & \blacksquare & \\ \hline & & \blacksquare & \blacksquare \\ \hline \blacksquare & \blacksquare & \blacksquare & \\ \hline 2 & 2 & 0 & 1 \\ \hline \end{array}
 \end{array}$$

さらに,

$$\begin{array}{ccc}
 H_0 = \begin{array}{|c|c|c|c|} \hline \blacksquare & \blacksquare & & \\ \hline & & \blacksquare & \blacksquare \\ \hline & & \blacksquare & \blacksquare \\ \hline \end{array} &
 H_1 = \begin{array}{|c|c|c|c|} \hline \blacksquare & & \blacksquare & \\ \hline & \blacksquare & & \blacksquare \\ \hline & \blacksquare & & \blacksquare \\ \hline \end{array} &
 H_2 = \begin{array}{|c|c|c|c|} \hline \blacksquare & & & \blacksquare \\ \hline & \blacksquare & \blacksquare & \\ \hline & \blacksquare & \blacksquare & \\ \hline \end{array}
 \end{array}$$

とおく。これだけで  $S(12,6,5)$  の構造を与えるに十分である。正確には, これらに対応する  $F_3$  上の 12 次元のベクトルを以下のように与えると, ternary Golay code  $C_{12}$  が生成される。

$$\begin{array}{ccc}
 & H_{(0,1)} \rightarrow \begin{array}{|c|c|c|c|} \hline 2 & 0 & 0 & 0 \\ \hline 1 & 1 & 1 & 1 \\ \hline 1 & 0 & 0 & 0 \\ \hline \end{array} & H_{(0,2)} \rightarrow \begin{array}{|c|c|c|c|} \hline 2 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 \\ \hline 1 & 1 & 1 & 1 \\ \hline \end{array} \\
 H_{(1,0)} \rightarrow \begin{array}{|c|c|c|c|} \hline 0 & 2 & 0 & 0 \\ \hline 1 & 1 & 0 & 1 \\ \hline 0 & 1 & 1 & 0 \\ \hline \end{array} & H_{(1,1)} \rightarrow \begin{array}{|c|c|c|c|} \hline 0 & 0 & 2 & 0 \\ \hline 1 & 1 & 1 & 0 \\ \hline 0 & 0 & 1 & 1 \\ \hline \end{array} & H_{(1,2)} \rightarrow \begin{array}{|c|c|c|c|} \hline 0 & 0 & 0 & 2 \\ \hline 1 & 0 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 \\ \hline \end{array} \\
 H_{(2,0)} \rightarrow \begin{array}{|c|c|c|c|} \hline 0 & 2 & 0 & 0 \\ \hline 0 & 1 & 1 & 0 \\ \hline 1 & 1 & 0 & 1 \\ \hline \end{array} & H_{(2,1)} \rightarrow \begin{array}{|c|c|c|c|} \hline 0 & 0 & 0 & 2 \\ \hline 0 & 1 & 0 & 1 \\ \hline 1 & 0 & 1 & 1 \\ \hline \end{array} & H_{(2,2)} \rightarrow \begin{array}{|c|c|c|c|} \hline 0 & 0 & 2 & 0 \\ \hline 0 & 0 & 1 & 1 \\ \hline 1 & 1 & 1 & 0 \\ \hline \end{array} \\
 H_0 = \begin{array}{|c|c|c|c|} \hline 2 & 2 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 1 & 1 \\ \hline \end{array} & H_1 = \begin{array}{|c|c|c|c|} \hline 2 & 0 & 2 & 0 \\ \hline 0 & 1 & 0 & 1 \\ \hline 0 & 1 & 0 & 1 \\ \hline \end{array} & H_2 = \begin{array}{|c|c|c|c|} \hline 2 & 0 & 0 & 2 \\ \hline 0 & 1 & 1 & 0 \\ \hline 0 & 1 & 1 & 0 \\ \hline \end{array}
 \end{array}$$

この構成法については [CS]11 章, [2] に詳しい。

なお, あとの話のためには  $\Delta$  の元の名前をつけておく方が良い。今までの話に加え,  $\Delta$  の長方形の 4 つの列には  $\{\infty\} \cup F_3$  という index をつけることにして

$$\Delta = \{x_a^{(n)} \mid a \in F_3, n \in \{\infty\} \cup F_3\}$$

$$\begin{array}{|c|c|c|c|} \hline
 x_0^{(\infty)} & x_0^{(0)} & x_0^{(1)} & x_0^{(2)} \\
 x_1^{(\infty)} & x_1^{(0)} & x_1^{(1)} & x_1^{(2)} \\
 x_2^{(\infty)} & x_2^{(0)} & x_2^{(1)} & x_2^{(2)} \\
 \hline
 \end{array}$$

と表されているものとする。

## 2.3 Transitive Extensions

$M_9 \subset A_6.2 \cong M_{10} \subset M_{11} \subset M_{12}$  という拡大である。デザインの言葉で言うなら affine 平面  $Af(F_3^2)$  (すなわち  $S(9,6,2)$ ) を順に拡大して  $S(12,6,5)$  を作ることに相当する。

[23],[21] では、(群論的に記述しやすいのか) まず  $F_9$  から始めて可移拡大を構成してから、デザインの記述をしている。

[7] の構成も、見掛けは異なるが同等の物だと言って良いと思う。

以下の話に不要であるので深入りはしないが、この構成法から自然に得られる記号の付け方が後で役に立つので、ここで導入しておこう。

前節の話と区別するために、12 点集合を  $\bar{\Delta}$  で表す。これを

$$\begin{aligned}\bar{\Delta} &:= Af(F_3^2) \cup F_3 \\ &= \{(a,b) \mid a,b \in F_3\} \cup \{0,1,2\}\end{aligned}$$

とおくのである (引用した文献とは若干異なる)。

前節のように MINIMOG ( $3 \times 4$ ) で表示しておく：

0	(0,0)	(0,1)	(0,2)
1	(1,0)	(1,1)	(1,2)
2	(2,0)	(2,1)	(2,2)

## 3 $M_{12}$ と $M_{24}$

### 3.1 $M_{24} \rightarrow M_{12}$

$(\Omega, \mathcal{O})$  を Steiner System  $S(24,8,5)$  とし、dodecade をひとつ固定し、それを  $\Delta$  とする。このとき、

$$\mathcal{H} = \{\Delta \cap O \mid O \in \mathcal{O}, |\Delta \cap O| = 6\}$$

とおくと、 $(\Delta, \mathcal{H})$  は  $S(12,6,5)$  になる。

Dodecade の 1 例を MOG で表しておく。

■	■	■	

### 3.2 $M_{12} \rightarrow M_{24}$

今述べたことの逆を行いたいわけである。

そこで、 $\Delta$  とそのコピー  $\bar{\Delta}$  の和集合として  $\Omega$  を定義する。そして  $(\Delta, \mathcal{H})$  の hexad  $H$  に対し  $\bar{\Delta}$  のある 2 元  $a, b$  を付け加えることにより octad  $H \cup \{a, b\}$  を構成する方法を与えた

いわけである。ここで、 $\Delta \setminus H$  も hexad であり octad を作るには、同じ 2 元  $a, b$  を加えればよいことを注意しておく。また、数を比べてみれば (hexad の総数)  $= 132 = 2 \times \binom{12}{2}$  であったから、 $\mathcal{H}$  と  $\Delta$  の 2 点集合全体との間に 2:1 対応が存在するというのは十分うなずける話であろう。

ここでは、[CS]11 章 17 節に従って、この 2:1 対応のひとつの (奇跡的に簡単な) 例を紹介しよう。

$\Delta = \{0, 1, 2, \dots, 10, 11\} \subset \mathbb{Z}$  とおき、総和が 21 になる  $\Delta$  の 6 元集合全体を考える：

$$\Delta_{21} := \left\{ S \subset \Delta \mid |S| = 6, \sum_{n \in S} n = 21 \right\}$$

$\Delta_{21}$  の中身を列挙しておこう。

$$\begin{aligned} H_{0,1} &:= \{ 1 \ 2 \ 3 \ 4 \ 5 \ 6 \} \\ H_{1,2} &:= \{ 0 \ 1 \ 2 \ 3 \ 7 \ 8 \} \\ H_{2,3} &:= \{ 0 \ 1 \ 2 \ 4 \ 5 \ 7 \} \\ H_{3,4} &:= \{ 0 \ 1 \ 3 \ 4 \ 6 \ 7 \} \\ H_{4,5} &:= \{ 0 \ 1 \ 2 \ 3 \ 5 \ 10 \} \\ H_{5,6} &:= \{ 0 \ 1 \ 2 \ 4 \ 6 \ 8 \} \\ H_{6,7} &:= \{ 0 \ 2 \ 3 \ 4 \ 5 \ 7 \} \\ H_{7,8} &:= \{ 0 \ 1 \ 2 \ 3 \ 6 \ 9 \} \\ H_{8,9} &:= \{ 0 \ 1 \ 3 \ 4 \ 5 \ 8 \} \\ H_{9,10} &:= \{ 0 \ 1 \ 2 \ 5 \ 6 \ 7 \} \\ H_{10,11} &:= \{ 0 \ 1 \ 2 \ 3 \ 4 \ 11 \} \end{aligned}$$

このとき奇妙な性質として次が成り立っている：

$$|H_{i,i+1} \cap H_{j,j+1}| = \begin{cases} 3 & (|i-j|=1) \\ 4 & (|i-j|>1) \end{cases}$$

次に、 $\Delta$  の dual として  $\bar{\Delta} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{10}, \bar{11}\}$  とおき

$$O_i := H_{i,i+1} \cup \{\bar{i}, \overline{i+1}\}$$

と定める。このとき、

$$|O_i \cap O_j| = 4 \ (i \neq j)$$

が成り立ち、 $\Omega := \Delta \cup \bar{\Delta}$  とおくと、

$$\langle O_0, O_1, \dots, O_{10}, \Delta \rangle \subset \mathcal{P}(\Omega)$$

が Golay code  $\mathcal{C}_{24}$  と同型になる。



### 3.3 $M_{12} \rightarrow M_{24}$ (II)

ここでは、後(6節)で必要となる形の構成を与える。

まず  $\Delta$  は 2.2 節で、その dual  $\bar{\Delta}$  は 2.3 節で定義されたものとする。このとき、 $\Omega := \Delta \cup \bar{\Delta}$  を MOG の記法で

$x_0^{(\infty)}$	$x_1^{(\infty)}$	$x_2^{(\infty)}$	0	1	2
(0, 0)	(2, 0)	(1, 0)	$x_0^{(0)}$	$x_1^{(1)}$	$x_2^{(2)}$
(0, 2)	(2, 2)	(1, 2)	$x_1^{(0)}$	$x_2^{(1)}$	$x_0^{(2)}$
(0, 1)	(2, 1)	(1, 1)	$x_2^{(0)}$	$x_0^{(1)}$	$x_1^{(2)}$

と並べることができる。

前節と同様に  $S(24, 8, 5)$  の構造を定義する。 $\Delta$  の hexad と  $\bar{\Delta}$  の 2 点集合を組み合わせる octad を作ってやればよいが、2.2 節の記号を用いると

$$\begin{aligned} O_{(a,b)} &:= H_{(a,b)} \cup \{(0,0), (a,b)\} \quad ((a,b) \neq (0,0)) \\ O_i &:= H_i \cup \{(0,0), i\} \end{aligned}$$

が octad であると定めればよい。

## 4 The Conway Group $Co.1$

Conway 群  $Co.1$  は Leech lattice の全自己同型群として定義される ([1])。この Leech lattice  $\Lambda$  は、24 次元の even unimodular lattice でルートを含まないものとして特徴づけられる。すなわち

24 次元 :  $\Lambda \subset \mathbb{R}^{24} = \mathbb{R}^\Omega$  (座標の index が  $\Omega$  であると考え)

even : 任意の  $v \in \Lambda$  に対し  $\|v\|^2 = (v, v)$  は偶数

unimodular :  $\Lambda = \Lambda^\perp := \{x \in \mathbb{R}^{24} | (x, v) \in \mathbb{Z} (\forall v \in \Lambda)\}$

ルートを含まない :  $\Lambda_1 = \emptyset$

をみtas。ただし、自然数  $i$  に対し、 $\Lambda_i := \{v \in \Lambda | \|v\|^2 = 2i\}$  とおき、 $\Lambda_1$  のベクトルを特に  $\Lambda$  のルートとよぶ。

### 4.1 The Golay Code

Euclid 空間  $\mathbb{R}^\Omega$  の直交基底を

$$e_i := \frac{1}{\sqrt{8}}(4, 0^{23})$$

で定義する。 $\|e_i\|^2 = 2$  である。さらに  $X \subset \Omega$  に対し、

$$e_X := \sum_{i \in X} e_i$$

とおく。このとき、Leech lattice  $\Lambda$  は Golay code を用いて、次のように定義される。

$$\Lambda = \sum_{X \in \mathcal{C}_{24}} \mathbb{Z} \frac{1}{2} e_X + \sum_{i \in \Omega} \mathbb{Z} \left( \frac{1}{4} e_\Omega - e_i \right)$$

定義に現れたベクトルを成分表示しておく

$$\begin{aligned} \frac{1}{2} e_X &= \frac{1}{\sqrt{8}} (2^{|X|}, 0^{24-|X|}) \\ \frac{1}{4} e_\Omega - e_i &= \frac{1}{\sqrt{8}} (-3^1, 1^{23}) \end{aligned}$$

となる。ただし、ベクトルの大まかな型を示すために同じ成分の個数を右上に記入した。以下のようなベクトルもまた  $\Lambda$  に含まれることが見て取れる：

$$\frac{1}{\sqrt{8}} ((\pm 4)^2, 0^{22}), \frac{1}{\sqrt{8}} (8, 0^{23}) \quad (\pm 4, 8 \text{ の位置はそれぞれ任意})$$

ここでは、 $e_i$  達を固定されたものとして定義したが、実際には次のような状況になっている。すなわち、任意の  $u \in \Lambda_4$  に対し、集合

$$\{v \in \Lambda_4 \mid u - v \in 2\Lambda\}$$

は 48 個のベクトルからなるからそれを適当な index と符号の付け方で

$$\{\pm 2f_i\}_{i \in \Omega}$$

とおくと、 $f_i$  達は  $\|f_i\|^2 = 2$  をみたす直交基底となり

$$\Lambda = \sum_{X \in \mathcal{C}_{24}} \mathbb{Z} \frac{1}{2} f_X + \sum_{i \in \Omega} \mathbb{Z} \left( \frac{1}{4} f_\Omega - f_i \right)$$

となる。 $f_i$  達を Leech lattice の 2-frame とよぶ。定義より、 $f_i \in \frac{1}{2}\Lambda$  である。

一般的な内容を含む文献として [15], [20] を挙げておく。

## 4.2 The Niemeier Lattices

$N$  を 24 次元の even unimodular lattice とする。すでに述べたように、 $N_1 := \{v \in N \mid \|v\|^2 = 2\} = \emptyset$  ならば  $N$  は Leech lattice と同型である。この条件を仮定しない分類が Niemeier によってなされており、それによると  $N$  は 24 通りの可能性があって、それぞれ  $N_1$  の形から特徴づけられ、

$$\begin{aligned} N_1 \cong \emptyset, A_1^{24}, A_2^{12}, A_3^8, A_4^6, D_4^6, A_5^4 D_4, A_6^4, A_7^2 D_5^2, A_8^3, D_6^4, A_9^2 D_6, E_6^4, \\ A_{11} D_7 E_6, A_{12}^2, D_8^3, A_{15} D_9, D_{10} E_7^2, A_{17} E_7, D_{12}^2, A_{24}, E_8^3, D_{16} E_8 \text{ or } D_{24} \end{aligned}$$

である。ここで、 $A_n, D_n, E_n$  は spherical type のルート系をあらわし、 $X_n^m$  とは  $X_n$  の  $m$  個の直和を意味する。

24 次元の even unimodular lattice  $N$  を総称して Niemeier lattice と呼ぶ。分類については Venkov による平易な証明が [CS]18 章にある。

Leech lattice 以外の 23 種類の Niemeier lattice から Leech lattice を構成する Conway-Sloane による "twenty-three constructions" が [CS]24 章にある。

### 4.3 The Lorentzian Lattice

2次元の Lorentzian lattice  $U$  を

$$U \cong \mathbb{Z} \oplus \mathbb{Z} \quad ((a, b), (c, d)) = -ad - bc$$

により定義する。この  $U$  と Leech lattice との直和

$$L := \Lambda \oplus U$$

は 26 次元の even unimodular Lorentzian lattice となる。ここで、 $U$  の長さ 0 のベクトル  $u = (1, 0)$  または  $(0, 1)$  に対し、

$$\Lambda \cong (u^\perp \cap L) / \langle u \rangle$$

であることに注意されたい。

これを利用した Leech lattice の (奇跡的に簡単な) 構成法をひとつだけ挙げておく ([CS]26 章)。すなわち、 $L$  を  $\Lambda$  と無関係に定義しておいて、ある  $u$  から上記のように  $\Lambda$  を構成するというものである。

$$L := \left\{ (x_0, \dots, x_{24}; x_{25}) \mid \begin{array}{l} \sum_{i=0}^{24} x_i - x_{25} \in 2\mathbb{Z}, \\ \forall x_i \in \mathbb{Z} \text{ or } \forall x_i \in \mathbb{Z} + \frac{1}{2} \end{array} \right\}$$

とおき、内積を

$$((x_i), (y_i)) := \sum_{i=0}^{24} x_i y_i - x_{25} y_{25}$$

定義すると、 $L$  は 26 次元の even unimodular Lorentzian lattice になる。

$$w := (0, 1, 2, \dots, 23, 24; 70) \in L$$

は長さ 0 であることが確かめられ、さらに、

$$\Lambda \cong (w^\perp \cap L) / \langle w \rangle$$

となる。

さて、26 次元の even unimodular Lorentzian lattice は同型を除いて一意であることが知られている。従って、任意の Niemeier lattice  $N$  に対し

$$L = \Lambda \oplus U \cong N \oplus U$$

である。従って、長さ 0 のある元  $u \in L$  により

$$N \cong (u^\perp \cap L) / \langle u \rangle$$

となる。このとき、 $\tilde{N} := u^\perp \cap L$  とおくと  $\tilde{N}_1$  は affine type ルート系 (例えば  $\tilde{A}_1^{24}, \tilde{A}_2^{12}, \tilde{E}_6^4$  など) をなす。

以下 [11] に従って, Leech root 並びに Leech glue root を説明する。

まず, Lorentzian lattice  $L = \Lambda \oplus U$  の

$$(\alpha, 1, \frac{(\alpha, \alpha) - 2}{2}) \quad \alpha \in \Lambda$$

の形のベクトルはすべてルートである。これらを特に Leech root とよぶことにする。 $N$  (または  $\tilde{N}$ ) の Leech root 全体は  $N_1$  (または  $\tilde{N}_1$ ) の基本ルート系をなすという著しい事実がある。

(例)  $\tilde{N}_1 = \tilde{A}_1^{24}$  の場合,  $\tilde{N}$  の Leech root は  $\pm 1$  倍を除けば 48 個のベクトルを含み, それらは互いに直交する 24 組に分かれる。これを  $\{\alpha_i, \beta_i\}$  と表し, 添え字  $i$  は  $\Omega$  を動くものとする。各組の 2 つのベクトルは下図のような Dynkin diagram で表現できる。

$$\alpha_i \bullet \text{---} \bullet \beta_i$$

ここで

$$\alpha_i = (a_i, 1, \frac{(\alpha, \alpha) - 2}{2}), \quad \beta_i = (b_i, 1, \frac{(\beta, \beta) - 2}{2})$$

とおくことにする。 $(\alpha_i, \beta_i) = -2$  であるから,

$$e_i = \frac{1}{2}(a_i - b_i) \in \Lambda$$

とおくと,  $e_i$  達は  $\|e_i\|^2 = 2$  をみたし Leech lattice  $\Lambda$  の 2-frame になり,

$$\Lambda = \sum_{X \in \mathcal{C}_{24}} \mathbb{Z} \frac{1}{2} e_X + \sum_{i \in \Omega} \mathbb{Z} (\frac{1}{4} e_\Omega - e_i)$$

となる。

次に, Leech glue root を説明しよう。

affine type  $\tilde{N}_1$  の (Leech root 全体のなす) 基本ルート系を  $\Phi$  とおく。 $r \in \Phi$  に対し,  $\Phi \setminus \{r\}$  が spherical type であるとき  $r$  を extended root と呼ぶことにする。 $\tilde{N}_1 = \tilde{A}_1^{24}, \tilde{A}_2^{12}$  の場合は, その Leech root すべてが extended root である。

また,  $\tilde{N}_1$  は 1 次元の totally isotropic vector を含むが, そのうち primitive な (基本ルートの正整数係数結合で表され, 係数たちの最大公約数が 1 である) ものを  $w_N$  と表すことにする。

Leech root  $s$  が  $\tilde{N}$  の Leech glue root であるとは,  $(s, w_N) = -1$  が成り立つことを意味する。このとき  $s$  は, 基本ルート系  $\Phi$  の各連結成分の extended root のうち, ただひとつ (仮に  $r$  とする) について  $(s, r) = -1$  となり他とは直交する。

(例)  $\tilde{N}_1 = \tilde{A}_1^{24}$  の場合, Leech glue root は  $2^{12}$  個存在する。先ほどの  $\{\alpha_i, \beta_i\}$  の代わりに  $\{0_i, 1_i\}$  という名前をうまく付けると, ひとつの Leech glue root について, 直交しないルートの記号 (0 か 1) を並べていくことで 24 次元のベクトル ( $F_2$  上と見る) を作ることで Golay code のベクトル全体が現れる。

$\tilde{N}_1 = \tilde{A}_2^{12}$  の場合は, 同じようにすれば ternary Golay code が現れる。

#### 4.4 $E_8$ -approach

Leech lattice の構成として Lepowsky-Meurman [16] による  $E_8$ -approach と呼ばれるものがある。これは Niemeier lattice のひとつ  $E_8^3$  が Leech lattice の sublattice になるという事実から始まるものである。ここでは、説明は省略する。

### 5 The Monster $M$

モンスターの構成としては、ある種の「代数」の全自己同型群としてとらえるものと、生成元と関係式によるものがある。

#### 5.1 Griess Algebra と Monster Vertex Operator Algebra

モンスターの最小次数の既約表現は 196,833 次である。ここに自明な 1 次の表現空間を加えた 196,834 次の空間に可換な非結合的な代数の構造を入れたものを Griess 代数といい、 $M$  はその全自己同型群になる ([10],[3])。その構成には  $C := (2_+^{1+24})(Co.1)$  という形の 2-local 極大部分群  $C$  が重要な役割を果たしている。この部分群の作用の下では 196,884 次の空間は

$$196,834 = 300 + 98,280 + 98,304$$

の形に分解される（「既約」ということなら 300 は  $1 + 299$  となる）。それぞれの部分空間（特にその次元）は、 $C$  に関する言葉で記述できる。

$$\begin{aligned} 300 &= \binom{24}{2} + 24 = \dim S^2(\mathbf{R} \otimes \Lambda) \\ 98,280 &= \frac{1}{2}|\Lambda_2| \\ 98,304 &= 24 \times 2^{12} \\ &= \dim(\mathbf{R} \otimes \Lambda) \times \dim I(2_+^{1+24}) \end{aligned}$$

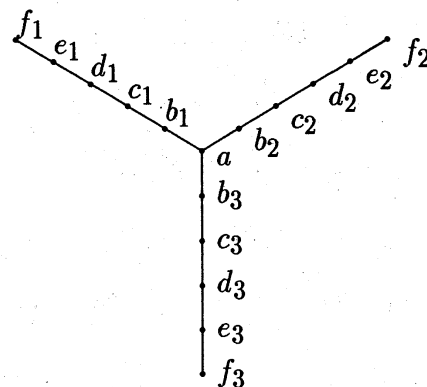
ただし、 $I(2_+^{1+24})$  は  $2_+^{1+24}$  の唯一の線形でない既約表現空間を表す。

Monster Vertex Operator Algebra は、いわゆる Moonshine 予想の答として得られたもので、無限個の積を持つ次数付きの無限次元代数で Griess 代数を homogeneous な部分代数として含んでいる ([9])。

ここではこれ以上立ち入らない。続く宮本氏による稿の中に、もう少し詳しい記述がある。

#### 5.2 $Y$ -presentation

まず  $Y_{555}$  とは、次のような図形である：



これを Coxeter diagram として、群の生成元と基本関係式と見る。すなわち、diagram の点は生成元に、辺は2つの元の積に対する関係式を与えていると考えるのであるが、各生成元は  $x^2 = 1$  をみたし、積  $xy$  については、対応する点が結ばれているときには  $(xy)^2 = 1$ 、結ばれていないときには  $(xy)^3 = 1$  であることを意味するものとする。

この  $Y_{555}$  から定義される群は無限群になる。これに簡単な関係式を1つ加えることで、Monster と位数2の群の Wreath 積  $M \wr 2$  (これを Bimonster と呼ぶ) が得られるというのが、いわゆる Y-presentation である ([12], [18], [19])。

$$M \wr 2 \cong \langle Y_{555}, (ab_1c_1ab_2c_2ab_3c_3)^{10} = 1 \rangle$$

このとき、 $M$  はひとつの生成元の中心化群として得られる。生成元と関係式という記述としては Bimonster と同様に

$$M \cong \langle Y_{553}, (ab_1c_1ab_2c_2ab_3c_3)^{10} = 1 \rangle$$

となる。ただし、 $Y_{553}$  とは  $Y_{555}$  から  $e_3, f_3$  を除いた図形である。

次に 26 node theorem について述べる。これは、Bimonster の上記の16個の生成元のほかに10個の元をとることにより、驚嘆すべききれいな関係式をみたされるというものである ([4], [5])。

#### 定理 (The 26 node theorem)

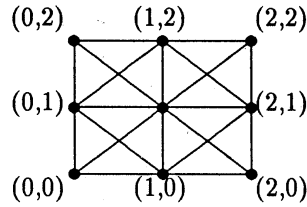
Bimonster  $M \wr Z_2$  の26個の involutions で、位数3の射影平面の incidence graph (射影平面の点と直線 (13個ずつ) を graph の点として、点が直線上にあるとき点と直線を辺で結んだもの) が与える関係式をみたすものが存在する。

Monster  $M$  の場合は21個の involutions で、位数3のアフィン平面から得られる関係式をみたす、ということになる。

## 6 21 Involutions

この節では、 $M$  の21個の involutions と同じ関係式をみたす Lorentzian lattice  $L$  のルートに関する reflections を構成する。ルート  $a$  に関する reflection を  $r_a$  と書くことにする

と,  $(a, b) = 0$  が  $|r_a r_b| = 2$  を  $(a, b) = -1$  が  $|r_a r_b| = 3$  を意味している。我々の目的はそのような関係を持つ 21 個のルートを求めることである。

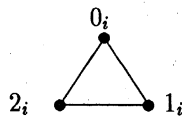


21 個のルートをアフィン平面の用語に合わせて 9 個の points と 12 個の lines と呼ぶことにする。

この”12”という数字の記述に  $S(12, 6, 5)$ ,  $M_{12}$  が使われる。

まずは, 宮本 [17] に従って 21 個のルートを構成しよう。

Lorentzian lattice  $L$  において, Niemeier lattice から得られる affine type のルート系  $\tilde{N}_1$  として  $\tilde{A}_2^{12}$  型のものをとる (4.3 節参照)。



このとき Leech glue root の全体は ternary Golay code と対応しており, 特に, 次のような Leech glue root が存在する。

$$\begin{aligned} s &= (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \\ r_0 &= (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \\ r_1 &= (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \\ r_2 &= (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \\ r_3 &= (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \end{aligned}$$

ただし  $r = (n(1), n(2), \dots, n(12))$  とは,

$$(r, n(i)_i) = -1, (r, m_i) = 0 \quad (m \neq n(i) \in F_3 = \{0, 1, 2\})$$

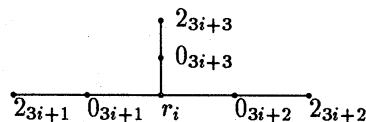
を意味するものとする。

このとき, さらに  $s, r_i$  達の関係も知ることができて

$$(r_i, r_j) = 2\delta_{i,j}, (r_i, s) = -1$$

が成り立っている。

そこで,  $0_i, 2_i$  達と  $r_j$  達のなす diagram を作ってみると,



となることがわかる。すなわち、 $\tilde{E}_6^4$  型の affine diagram であり、これがある Niemeier lattice から 4.3 節のように得られるものであることも（一般論として）わかる。そこで、その Leech glue root 全体を  $p_1, \dots, p_9$  とおくと  $\{p_i\}_{i=1, \dots, 9}, \{q_j\}_{j=1, \dots, 12}$  が位数 3 のアフィン平面から得られる関係式をみたしているのである。

さて、ここで注意を喚起したいことがある。それは、今の話を  $\tilde{A}_2^{12}$  から始めたのか？ということである。実際、21 個のベクトルの構成だけならば  $\tilde{E}_6^4$  だけで足りる話である。 $\tilde{A}_2^{12}$  から始めた理由は、（そして、それは宮本氏の結果のひとつの Key Point であると思われるのだが） $s$  というベクトルを自然に登場させることにあった。この  $s$  は次をみたしている。

$$(p_i, s) = -2 \quad (\forall p_i)$$

そこで、 $p_i$  をひとつ選んで  $p = p_i$  とおく。 $p, s$  のみたす関係は  $\tilde{A}_1$  の関係である。すると、ここから Lorentzian lattice の一般論から affine type  $\tilde{A}_1^{24}$  のルート系が得られる。そして、4.3 節で述べたように Leech lattice の 2-frame が定まり、

$$\Lambda = \sum_{X \in C_{24}} \mathbb{Z} \frac{1}{2} e_X + \sum_{i \in \Omega} \mathbb{Z} \left( \frac{1}{4} e_\Omega - e_i \right)$$

という座標表示が定まる ( $e_1 = p - s$ )。

宮本氏の結果というのは、21 個のベクトルに対応する Monster algebra の 21 個の自己同型を、この座標表示を用いて定義して、さらにそれらの関係式が確認される、というものである。

それでは、定まった座標表示によって  $\{p_i\}_{i=1, \dots, 9}, \{q_j\}_{j=1, \dots, 12}$  を実際に表示してみることにする。正確に言うと、 $p_i = (\bar{p}_i, 1, \frac{(\bar{p}_i, \bar{p}_i) - 2}{2})$   $q_j = (\bar{q}_j, 1, \frac{(\bar{q}_j, \bar{q}_j) - 2}{2})$  と表したときの  $\bar{p}_i, \bar{q}_j$  達を以下に与えよう。また、簡単のため  $s = (0, 1, -1)$  としておく。

まず、2-frame の index  $\Omega = \Delta \cup \bar{\Delta}$  は 3.3 節のように定まっているものとする。この index が明確になるように Lorentzian lattice の 2-frame を表す記号をあらためて

$$\begin{aligned} e_i^{(n)} &\leftrightarrow x_i^{(n)} \in \Delta \\ e_{(a,b)} &\leftrightarrow (a, b) \in \bar{\Delta} \\ e_i &\leftrightarrow i \end{aligned}$$

とする。MOG の形に書いておく。

$e_0^{(\infty)}$	$e_1^{(\infty)}$	$e_2^{(\infty)}$	$e_0$	$e_1$	$e_2$
$e_{(0,0)}$	$e_{(2,0)}$	$e_{(1,0)}$	$e_0^{(0)}$	$e_1^{(1)}$	$e_2^{(2)}$
$e_{(0,2)}$	$e_{(2,2)}$	$e_{(1,2)}$	$e_1^{(0)}$	$e_2^{(1)}$	$e_0^{(2)}$
$e_{(0,1)}$	$e_{(2,1)}$	$e_{(1,1)}$	$e_2^{(0)}$	$e_0^{(1)}$	$e_1^{(2)}$

以上の記号の下で、 $\bar{p}_i, \bar{q}_j$  達は次のように表される。2-frame を固定しているから、座標の並べ替えと（許される） $\pm 1$  倍（すなわち、Conway 群の極大部分群  $2^{12} \cdot M_{24}$  の作用）を除けば、この表示は一意に定まるものである。（右側に成分表示の型を示しておいた。）



$\{\bar{p}_i\}$  (9 points)

$$2e_{(0,0)} \quad \frac{1}{\sqrt{8}}(8, 0^{23})$$

$$\frac{3}{2}e_{(0,0)} + \frac{1}{2}e_{(a,b)} + \frac{1}{2} \sum_{x_i^{(n)} \in H_{a,b}, n \neq \infty} e_i^{(n)} - \frac{1}{2} \sum_{x_i^{(\infty)} \in H_{a,b}} e_i^{(\infty)} \quad \frac{1}{\sqrt{8}}(6, \pm 2^7, 0^{16})$$

ただし,  $(a, b) \in F_3^2 \setminus \{(0, 0)\}$  である。0 でない成分の位置は octad  $O_{a,b}$  で,  $(0, 0)$  の部分に 6 がある。

$\{\bar{q}_j\}$  (12 lines)

$$e_{(0,0)} + e_i^{(n)} \quad (i \in F_3 \setminus \{0\}, n \in F_3 \cup \{\infty\}) \quad \frac{1}{\sqrt{8}}(4^2, 0^{22})$$

$$e_{(0,0)} - \frac{1}{2}e_X + \frac{1}{4}e_\Omega \quad \frac{1}{\sqrt{8}}(3, (-1)^7, 1^{16})$$

ただし,  $X$  とは  $\{x_1^{(\infty)}, x_2^{(\infty)}, (0, 0), (0, 1), (0, 2), 0, 1, 2\}$  または,  $k \in F_3 \cup \{\infty\}$  に対する  $\{x_0^{(k)}, x_a^{(\infty)} (a \in F_3), (0, 0), (1, k), (2, 2k), k\}$  という, 合わせて 4 つの octads のいずれかである。

## 7 補足

本文で全く触れることのできなかつた話はいくつも残っている。例えば [8] は, カードのシャッフルという意外な観点から  $M_{12}$  の生成元が与えられるという印象的な事実を述べている。また, [13] は  $S(24, 8, 5), S(12, 6, 5)$  を統一的に構成するものであり, その difference pattern のアイデアは全ての Octads, Hexsads を (実際に) 書き下す際に有効である。そして [CS] には, もっともっと沢山の内容が詰まっている。

感じることは, 色々の構成法があるのは色々な数学が背景にあるということである。3.3 節の  $\Omega$  の元の名付け方も, 6 節の 21 involutions を与えようとする所から逆算して得られたものである。

新しい構成法がまだどこかにあって, そこから Monster の新しい (平易な) 構成法につながることを期待したい。

## 参考文献

- [1] J.H.Conway, Three lecture on exceptional groups, in "Finite simple groups", Academic Press, 1971, 215-247
- [2] J.H.Conway, Hexacode and Tetracode - MOD and MINIMOG, in "Computational Group Theory", 359-365
- [3] J.H.Conway, A simple construction for the Fischer-Griess monster group, Invent. Math. 79 (1985), 513-540.

- [4] J.H.Conway, S.P.Norton and L.H.Soicher, The Bimonster, the group  $Y_{555}$  and the Projective Plane of Order 3, in "Proceedings of Computers in algebra, Chicago, 1985", Dekker (1988), 27–50.
- [5] J.H.Conway and A.D.Pritchard, Hyperbolic reflections for the Bimonster and  $3Fi_{24}$ , in "Groups, Combinatorics and Geometry", Cambridge, 1992.
- [6] R.T.Curtis, A new combinatorial approach to  $M_{24}$ , Math. Proc. Cambridge Philos. Soc., 79 (1976), 25–42
- [7] R.T.Curtis, The Steiner System  $S(5, 6, 12)$ , the Mathieu Group  $M_{12}$  and the "Kitten", in "Computational Group Theory", 353–358
- [8] P.Diaconis, R.L.Graham, W.M.Kantor, The Mathematics of Perfect Shuffles, Advanced in Applied Math. 4 (1983), 175–196.
- [9] I.Frenkel, J.Lepowsky and A.Meurman, Vertex Operator Algebras and the Monster, Pure and Appl. Math. Vol. 134, Academic Press, Boston, 1988.
- [10] R.L.Griess, The Friendly Giant, Invent. Math. 69 (1982), 1–102.
- [11] K.Harada, M.L.Lang and M.Miyamoto, Sequential Construction of Niemeier Lattices and Uniqueness proof, to appear in J. Number Theory.
- [12] A.A.Ivanov, A geometric characterization of the Monster, in "Groups, Combinatorics and Geometry", Cambridge, 1992.
- [13] S.Iwasaki, An elementary and unified approach to the Mathieu-Witt systems, J. Math. Soc. Japan, 40-3 (1988), 393–414.
- [14] M.Kitazume, Code loops and even codes over  $F_4$ , J. Algebra 118 (1988), 140–149.
- [15] M.Kitazume, T.Kondo and I.Miyamoto, Even lattices and doubly even codes, J. Math. Soc. Japan 43 (1991), 67–87.
- [16] J.Lepowsky and A.Meurman, An  $E_8$ -approach to the Leech lattice and the Conway group, J. Alg. 77 (1982), 484–504.
- [17] M.Miyamoto, 21 involutions acting on the Moonshine module, J.Alg.175, 941–965 (1995)
- [18] S.Norton, Presenting the Monster?, Bull. Soc. Math. Belg. 62 (1990), 595–605.
- [19] S.Norton, Construction the Monster, in "Groups, Combinatorics and Geometry", Cambridge, 1992.

- [20] T.Tasaka, On even lattices of 2-squares type and self-dual codes, J. Fac. Sci. Univ. Tokyo Ser.IA 28 (1981), 701–704.
- [21] 大山 豪, 有限置換群, 裳華房.
- [22] 近藤 武, Mathieu 群と Conway 群, 講義録<sup>1</sup>.
- [23] 永尾 汎, 群とデザイン, 岩波書店.

---

<sup>1</sup>興味のある方は北詰までお問い合わせください。